N

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/774,102	01/31/2001	Jonathan S. Goldstone	Q60463	1078

7590 10/18/2004

SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
WASHINGTON, DC 20037-3213

EXAMINER	
KADING, JOSHUA A	
ART UNIT	PAPER NUMBER
2661	

DATE MAILED: 10/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/774,102	**Applicant(s)** GOLDSTONE, JONATHAN S.	
	Examiner Joshua Kading	**Art Unit** 2661	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☒ Claim(s) *4* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 January 2001* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Drawings

Figure 2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.121(d)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Claim 4 is objected to because of the following informalities: Line 4 states "client access the Internet". The word "to" should be inserted between the words "access" and "the", i.e. --client access to the Internet--. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 5-8, 10-13, 15-19, 21-23, and 25-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Yavatkar et al. (U.S. Patent 6,735,702 B1).

Regarding claim 1, Yavatkar discloses "a method for preventing bandwidth congestion on a network, said method comprising: providing at least one origination client connected to the Internet through respective connection points (col. 15, lines 4-11 where the fact that the "watchdog agent" is monitoring for attacks means that the attacks originate from some place and this place is connected to the network; it should further be noted that throughout Yavatkar, the network operates using IP/TCP); providing at least one destination server connected to the Internet (col. 15, lines 4-11 where the monitored nodes are the equivalent to destination servers); directing at least one request for connection from at least one of said origination clients to a target destination server over the Internet (col. 15, line 18 where as stated in applicant's specification, figure 2, a SYN/ACK is a type of request for connection); and automatically, upon detecting an overload condition of requests for connection, blocking the origination client, or clients, responsible for said overload condition from accessing the Internet through its, or their, respective connection point(s) (col. 17, lines 20-27)."

Regarding claim 2, Yavatkar discloses "a method as claimed in claim 1, wherein said connection point through which said origination client(s) is blocked from accessing the Internet, is a connection point which is physically closest to said origination client (col. 17, lines 20-27 where the fact that the attack is traced to a final node (even if it is not the exact source of the attack) means that connection point is the closest possible point to the origination client as can be traced, and that is what is blocked)."

Regarding claim 3, Yavatkar discloses "a method as claimed in claim 1, further comprising: communicating an IP address of said origination client(s) responsible for said overload condition to said connection point(s) (col. 18, lines 54-60 whereby reforming routing tables to not include the source of the attack the IP address of the origination client must be known and the routing tables of other nodes (connection points) must also be updated for the restructuring to take effect)."

Regarding claim 21, Yavatkar discloses "a method as claimed in claim 1, wherein one or more of said destination servers are protected by a respective firewall and wherein said detection of said overload condition is carried out by one of said respective firewalls (col. 17, lines 20-27)."

Regarding claim 22, Yavatkar discloses "a method as claimed in claim 1, wherein said detection of said overload condition is carried out by said target destination server (col. 15, lines 4-6 where the device operating the "watchdog agent" can be the target destination)."

Regarding claim 23, Yavatkar discloses "a method as claimed in claim 1, wherein said detection of said overload condition is carried out by a respective target router operable connected to said target destination server (col. 15, lines 4-7 where the "watchdog agent" can operate from a remote node connected to the target destination)."

Regarding claims 5 and 16, Yavatkar discloses "a method for preventing bandwidth congestion on a network, said method comprising: providing a destination site router connected to a destination site locally and also to an internet connection (col. 15, lines 4-11 where the fact that the "watchdog agent" is monitoring for attacks means that the attacks originate from some place and this place is connected to the network; it should further be noted that throughout Yavatkar, the network operates using IP/TCP); providing a plurality of origin site routers one or many of which may be connected to an attacking site, wherein each of said plurality of sites has a respective address associated with it (col. 15, lines 4-11 where the monitored nodes are the equivalent the site routers and it is inherent in the nodes that they each have their own address, if they didn't how would data get routed to them?); providing connectivity between said origin and destination routers to the Internet or other wide area networks (WAN) (col. 15, lines 4-11 where all nodes are connected to the Internet); detecting a bandwidth congestion at said destination site router, wherein said bandwidth congestion originates at said attacking site (col. 16, lines 22-25 where the "watchdog agent" is part of the destination router and it is inherent that the attack will originate from the attacking site); informing said origin site router and other intermediate routers within the Internet, or other WAN, of said bandwidth congestion and of an attacking address corresponding to said attacking site from which said bandwidth congestion originated (col. 18, lines 54-60); preventing said attacking address corresponding to said attacking site from being used to gain access to the internet or other WAN (col. 18, lines 54-60)."

Regarding claim 6, Yavatkar discloses "a method in accordance with claim 5, wherein said informing is performed automatically by said destination router (col. 16, lines 22-25)."

Regarding claim 7, Yavatkar discloses "a method in accordance with claim 5, wherein said informing is performed by human intervention (col. 16, lines 22-25)."

Regarding claim 8, Yavatkar discloses "a method in accordance with claim 5 further comprising: informing a plurality of remote routers connected to the Internet of said attacking address (col. 18, lines 56-60)."

Regarding claim 15, Yavatkar discloses "a method for preventing bandwidth congestion on a network, said method comprising: providing a destination site router connected to a destination site locally and also to an internet connection (col. 15, lines 4-11 where the fact that the "watchdog agent" is monitoring for attacks means that the attacks originate from some place and this place is connected to the network; it should further be noted that throughout Yavatkar, the network operates using IP/TCP);

providing a plurality of origin site routers one or many of which may be connected to an attacking site, wherein each of said plurality of sites has a respective address associated with it (col. 15, lines 4-11 where the monitored nodes are the equivalent the site routers and it is inherent in the nodes that they each have their own address, if they didn't how would data get routed to them?); providing connectivity between said origin and destination routers to the Internet or other wide area networks (WAN) (col. 15, lines 4-11 where all nodes are connected to the Internet); detecting a bandwidth congestion at a firewall connected to said destination site router, wherein said bandwidth congestion originates at said attacking site (col. 16, lines 22-25 where the "watchdog agent" is part of remote router that can use a firewall as stated in col. 17, lines 24-27; and it is inherent that the attack will originate from the attacking site); informing said origin site router and other intermediate routers within the Internet, or other WAN, of said bandwidth congestion and of an attacking address corresponding to said attacking site from which said bandwidth congestion originated (col. 18, lines 54-60); preventing said attacking address corresponding to said attacking site from being used to gain access to the internet or other WAN (col. 18, lines 54-60)."

Regarding claim 10, Yavatkar discloses "a network system that prevents bandwidth congestion on a network, said system comprising: a destination server connected to the Internet through a destination router (col. 15, lines 4-11 where the fact that the "watchdog agent" is monitoring for attacks means that the attacks originate from some place and this place is connected to the network; it should further be noted that throughout Yavatkar, the network operates using IP/TCP); an attack detector operable to detect a denial of service or other Internet-based attack (col. 16, lines 22-25 where the "watchdog agent" is used to detect the attack); an origination client connected to the Internet through an origination router, said origination client being operable to initiate a denial of service or other Internet-based attack (col. 15, lines 4-11 where the fact that the "watchdog agent" is monitoring for attacks means that the attacks originate from some place and this place is connected to the network and this site is capable of initiating an attack as read in col. 15, lines 7-11); wherein said attack detector is further operable to communicate an identity of said origination client to said origination router to prevent said origination client from being operable to continue said detected denial of service attack (col. 18, lines 54-60)."

Regarding claim 11, Yavatkar discloses "a network system according to claim 10, wherein said communication of said identity of said origination client occurs automatically upon detection of said denial of service or other Internet-based attack (col. 16, lines 22-25)."

Regarding claim 25, Yavatkar discloses "a network system in accordance with claim 10 wherein said attack detector is located within a firewall device located between said destination server and said origination client (col. 17, lines 20-27)."

Regarding claim 26, Yavatkar discloses “a network system in accordance with claim 10 wherein said attack detector is located within said destination server (col. 15, lines 4-6 where the device operating the “watchdog agent” can be the destination).”

Regarding claim 27, Yavatkar discloses “a network system in accordance with claim 10 wherein said attack detector is located within said destination router (col. 15, lines 4-6 where the device operating the “watchdog agent” can be the destination).”

Regarding claims 12 and 18, Yavatkar discloses “a network system that prevents bandwidth congestion on a network, said system comprising: an origin client router connected to a plurality of clients through an Internet connection, said plurality of clients including an attacking client, and wherein each of said plurality of clients has a respective address associated with it (col. 15, lines 4-11 where the fact that the “watchdog agent” is monitoring for attacks means that the attacks originate from some place and this place is connected to the network; it should further be noted that throughout Yavatkar, the network operates using IP/TCP); a destination site router connected to a destination server (col. 15, lines 4-11 where the monitored nodes are the equivalent to destination servers), said destination site router or firewall or client further comprising a bandwidth congestion detector operable to detect a bandwidth congestion condition (col. 16, lines 22-25 where the “watchdog agent” is used to detect the attack) and a communication device operable to communicate said bandwidth congestion condition and said addresses to said plurality of clients (col. 18, lines 54-60); a router-router connection between said origin client router and said destination site router, wherein said router-router connection provides a discrete amount of access bandwidth by which said client router and said destination site router can pass data traffic back and forth to each other (col. 15, lines 4-11 where the given nodes are all connected through the network; further it is inherent that there is a discrete amount of access bandwidth by which data can be transmitted, no link or network has unlimited bandwidth, therefore each link must have a given value for bandwidth); wherein said bandwidth congestion detector detects a bandwidth congestion condition originating at said attacking client and directed to said destination server and automatically informs said origin client router of said attacking client's respective address (col. 18, lines 54-60 where the attack is the result of the bandwidth congestion as stated in col. 15, lines 63-64), and wherein further, said origin client router prevents said address of said attacking client from causing further bandwidth congestion (col. 18, lines 54-60 whereby reforming the routing tables effectively prevents the address of attacking client from causing further congestion)."

Regarding claim 17, Yavatkar discloses "a network system that prevents bandwidth congestion on a network, said system comprising: an origin client router connected to a plurality of clients through an Internet connection, said plurality of clients including an attacking client, and wherein each of said plurality of clients has a respective address associated with it (col. 15, lines 4-11 where the fact that the "watchdog agent" is monitoring for attacks means that the attacks originate from some place and this place is connected to the network; it should further be noted that throughout Yavatkar, the network operates using IP/TCP); a destination site router connected to a destination server (col. 15, lines 4-11 where the monitored nodes are the equivalent to destination servers); a firewall connected to said destination server, said firewall comprising a bandwidth congestion detector operable to detect a bandwidth congestion condition (col. 16, lines 22-25 where the "watchdog agent" is used to detect the attack) and a communication device operable to communicate said bandwidth congestion condition and said addresses to said plurality of clients (col. 18, lines 54-60); a router-router connection between said origin client router and said destination site router, wherein said router-router connection provides a discrete amount of access bandwidth by which said client router and said destination site router can pass data traffic back and forth to each other (col. 15, lines 4-11 where the given nodes are all connected through the network; further it is inherent that there is a discrete amount of access bandwidth by which data can be transmitted, no link or network has unlimited bandwidth, therefore each link must have a given value for bandwidth); wherein said bandwidth congestion detector detects a bandwidth congestion condition originating at said attacking client and directed to said destination server and automatically informs said origin client router of said attacking client's respective address (col. 18, lines 54-60 where the attack is the result of the bandwidth congestion as stated in col. 15, lines 63-64), and wherein further, said origin client router prevents said address of said attacking client from causing further bandwidth congestion (col. 18, lines 54-60 whereby reforming the routing tables effectively prevents the address of attacking client from causing further congestion)."

Regarding claim 13, Yavatkar discloses "a system in accordance with claim 12, wherein said destination site router further informs a plurality of other intermediate routers within the Internet or shared WAN routers in addition to said origin client router (col. 18, lines 54-60)."

Regarding claim 19, Yavatkar discloses "a computer medium storing a program operable to perform the following functions (col. 15, lines 4-11 where the "watchdog agent" operates on nodes, i.e. the "watchdog agent" is a program used to detect problems in the network): detect an internet-based attack directed to a target server from an attacking client (col. 16, lines 22-25 where the "watchdog agent" is used to detect the attack); automatically communicate an identity of said attacking client to at least one router through which said attacking client is connected to the Internet (col. 18, lines 54-60)."

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al.

Regarding claim 24, Yavatkar discloses the method of claim 5. However, Yavatkar does not explicitly disclose "said preventing is performed until a human administrator intervenes after determining whether said attacking site should be permitted to gain access to the Internet." Although Yavatkar does not explicitly disclose the human administrator permitting access to the Internet, Yavatkar does strongly suggest this is the case (col. 6, lines 12-18 where the ability of a human operator to send commands to nodes, instructing the nodes how to behave strongly suggests a human operator has the capability to allow or prevent a given address from accessing a node). It would have been obvious to one with ordinary skill in the art at the time of invention to include the human operator allowing or preventing access to a given node for the purpose of allowing legitimate users to access the network while stopping malicious users from accessing the network. The motivation for not allowing malicious attacks to propagate through the network is to prevent network congestion and thus allow legitimate users to properly access the network (col. 15, lines 63-64).

Claims 4, 9, 14, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yavatkar et al. in view of Cox et al. (U.S. Patent 6,738,814 B1).

Regarding claims 4, 9, and 14, Yavatkar discloses the method of claim 1, the method of claim 5, and the system of claim 12. However, Yavatkar lacks what Cox discloses, "determining whether said blocked origination client should be permitted to gain access to the Internet (col. 4, lines 62-67 where the incoming address could still come from a blocked client and as such the address will be checked against a database to check validity); and permitting said blocked origination client access to the Internet if it is determined that said blocked origination client should be permitted access to the Internet (col. 4, line 67-col. 5, lines 1-3 where if the address is not on the list, that is it does not already have a connection setup or is not an attack, the connection is allowed)." It would have been obvious to one with ordinary skill in the art at the time of invention to include the allowing an address or client access to the network for the purpose of allowing a legitimate user access. The motivation for having to check for a valid address is to confirm that the client or user is no longer or not at all associated with an attack that will cause congestion.

Regarding claim 20, Yavatkar discloses the computer program of claim 19. Yavatkar further discloses, "prevent said attacking client from gaining access to the Internet (col. 17, lines 20-27)..." However, Yavatkar lacks what Cox discloses, "determine whether said attacking client is attempting to initiate an Internet-based attack (col. 4, lines 62-67 where the incoming address could still come from a blocked client and as such the address will be checked against a database to check validity); permit said attacking client to gain access to the Internet if it is determined that said attacking client is not attempting to initiate an Internet-based attack (col. 4, line 67-col. 5, lines 1-3 where if the address is not on the list, that is it does not already have a connection setup or is not an attack, the connection is allowed)." It would have been obvious to one with ordinary skill in the art at the time of invention to include the allowing an address or client access to the network for the purpose of allowing a legitimate user access. The motivation for having to check for a valid address is to confirm that the client or user is no longer or not at all associated with an attack that will cause congestion.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joshua Kading whose telephone number is (571) 272-3070. The examiner can normally be reached on M-F: 8:30AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kenneth Vanderpuye can be reached on (571) 272-3078. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Joshua Kading
Examiner
Art Unit 2661

October 15, 2004

KENNETH VANDERPUYE
PRIMARY EXAMINER